CLAIMS

1. A method of processing data, the method comprising:

receiving data from a network link;

replicating said data on board a network analyser card to produce at least two editions of the received data; and

writing said editions of the received data to an area of memory in a host that is directly accessible by a host application.

2. A method according to claim 1, comprising:

processing said editions of data stored in the said area of memory accessible by a host application, the processing comprising executing a different set of rules relating to intrusion detection on each edition.

3. A method according to claim 1 or 2, in which the data is replicated using hardware.

4. A method according to any of claims 1 to 3, in which the editions of the received data are provided as independent data streams.

5. A method according to any of claims 1 to 4, in which each of the at least two editions of said received data is buffered independently.

6. A method according to claim 4, in which each of the independent data streams is filtered according to desired criteria.

7. A method according to claim 4, in which different

filtering rules are applied to each of the editions of the received data.

8 A method according to any of claims 1 to 7, the method comprising:

writing the editions of the received data to an area of kernel memory of the host memory; and

providing to the host application an offset to enable location of the data by the host application in the kernel space of the memory.

9. A method according to claim 8, in which when data is written to the kernel space of the host memory a list of offsets with respect to a base address within kernel space is generated, the list of offsets serving to enable location of data packets within the kernel space with respect to the base address.

10. A method according to claim 9, comprising:

providing to an application for running in application space, an offset to enable location of the base address of the data within the kernel space.

11. A method according to claim 9 or 10, comprising:

providing to the application a list of offsets with respect to the offset of the base address.

12. A method according to any of claims 1 to 11, in which the data is received as data frames from a network link.

13. A method according to claim 12, comprising:

adding to substantially each of the received data frames a descriptor, the descriptor containing data

relating to the data frame to which it is attached.

14. A network analyser card for connection to a host and a network, the card comprising:

a receiver for receiving plural data frames from a network link;

data replication means for generating at least two replica editions of the received data frames; and

a descriptor adder configured and arranged to add a descriptor to substantially each of the data frames of each of the at least two replica editions of the received data frames, the descriptor including data about the data frame to which it is attached for use in processing of the data frame.

15. A network analyser card according to claim 14, comprising:

data writing means for writing the at least two replica editions of the received data frames to an area of host memory directly accessible by a host application.

16. A network analyser card according to claim 14 or 15, in which the descriptor includes data indicative of the length of a data frame to which it is attached.

17. A network analyser card according to any of Claims 14 to 16, in which the descriptor includes a timestamp indicative of the time at which the corresponding data frame was received at the network analyser card.

18. A network analyser card according to any of claims 14 to 17, wherein one or more of the data replication means, the descriptor adder and the data writing means is or are

arranged in hardware.

19. A network analyser card according to any of claims 14 to 18, the network analyser card being controllable to execute the steps of the method of any of claims 1 to 13.

20. A host for connection to a network, the host comprising:

a network analyser card for receiving data from the network;

a memory to receive at least two editions of the received data from the network analyser card; and

at least two processors for processing said editions of the received data, wherein the network analyser card is in accordance with any of claims 14 to 19.

21. A host according to claim 20, wherein each of the at least two processors is arranged to execute a different set of rules on each edition of the stored data.

22. A host according to claim 21, wherein the rules relate to intrusion detection.

23. An intrusion detection system, comprising a host according to any of claims 20 to 22, wherein the processors are arranged to execute rules of an intrusion detection system on data packets received by the host.